

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
v.	)	<b>Case No. 1:14CR230</b>
	)	
<b>MUNA OSMAN JAMA,</b>	)	
	)	
<b>and</b>	)	
	)	
<b>HINDA OSMAN DHIRANE,</b>	)	
	)	
<b>Defendants.</b>	)	

**DEFENDANTS’ JOINT MOTION TO SUPPRESS ELECTRONIC SURVEILLANCE  
OBTAINED WITHOUT A WARRANT AND WITHOUT A FINDING OF PROBABLE  
CAUSE OF CRIMINAL CONDUCT, AND FOR DISCLOSURE OF THE FISA  
APPLICATIONS TO DEFENSE COUNSEL**

COMES NOW the defendant, Muna Jama, by counsel, Whitney E.C. Minter, Assistant Federal Public Defender, and Jeremy C. Kamens, Acting Federal Public Defender, and defendant Hinda Dhirane, by counsel Alan Yamamoto, and hereby move this Court: (1) to suppress all interceptions made and electronic surveillance and physical searches conducted pursuant to the Foreign Intelligence Surveillance Act (hereinafter “FISA”), 50 U.S.C. §1801, et seq., and any fruits thereof, because the FISA surveillance was obtained and conducted in violation of FISA and the First and Fourth Amendments to the U.S. Constitution, and (2) for disclosure of the underlying applications for FISA warrants.

As an initial matter, disclosure of the FISA applications to defense counsel – who possess the requisite security clearances – is an essential prerequisite to an accurate determination of the legality of the FISA surveillance and due process in this case. Otherwise the defense will be unable to adequately represent the defendants, and the Court will not have the benefit of the defense

perspective on the key issues related to determining whether the FISA surveillance was lawful.

### **STATEMENT OF FACTS**

Muna Jama and Hinda Dhirane are charged in a twenty-one count Indictment with Conspiracy to Provide Material Support for Terrorism, in violation of 18 U.S.C. § 2339B (Count One); and Material Support of a Foreign Terrorist Organization in violation of 18 U.S.C. § 2339B (Counts Two through Twenty-One).

Both Ms. Jama and Ms. Dhirane were born in Somalia. The government of Somalia was overthrown in 1992, and the country descended into a decades-long series of armed conflicts that, in some form, have continued to the present. Ms. Jama's family was forced to flee the fighting in Mogadishu. They traveled to other towns within Somalia, but, within a year, were forced to leave the country altogether due to the instability. They then moved to Kenya where Ms. Jama was able to resume her schooling. After living in refugee camps for several years, Ms. Jama was able to immigrate to the United States with members of her extended family on a refuge visa.

Much of Somalia continues to suffer from instability and the absence of government control. Consequently, people in Somalia often seek assistance from their ex-patriot relatives and members of their community who are now living abroad.

The charges in this case stem from an allegation that Ms. Jama, Ms. Dhirane, and their co-defendants, transferred money to individuals in Somalia who were affiliated with *al Shabaab*, which was designated on February 26, 2008, as a Foreign Terrorist Organization. The Indictment alleges that over the course of two years, Ms. Jama and Ms. Dhirane transferred a total of approximately \$4,750.00, usually in \$100 to \$200 increments, to two individuals in Somalia and Kenya. The government alleges that these transactions were for the purpose of supporting *al Shabaab*.

Ms. Jama and Ms. Dhirani now move for suppression of any and all evidence obtained pursuant to the FISA electronic surveillance and physical searches, as well as disclosure of the underlying applications for FISA warrants.

### **Argument**

On July 23, 2014, the government filed a notice stating that it intends to offer into evidence “information obtained or derived from electronic surveillance and physical search pursuant to [FISA],” and discovery has revealed extensive products of surveillance pursuant to FISA.<sup>1</sup>

As detailed below, the interceptions and e-mails the government obtained pursuant to FISA should be suppressed because the surveillance and collection were conducted in violation of FISA, and of the First and Fourth Amendments. However, because defense counsel have not been provided with the underlying applications for the pertinent FISA warrants, this motion can only outline the possible bases for suppression for the Court to examine and consider.

#### **A. Background**

FISA, 50 U.S.C. §1801, *et seq.*, was enacted in 1978 in the wake of domestic surveillance abuses by federal law enforcement agencies as catalogued in Congressional Committee and Presidential Commission Reports.<sup>2</sup> The statute was designed to provide a codified framework

---

<sup>1</sup> The government has not provided notice that it conducted electronic surveillance pursuant to the 2008 Amendments to FISA. Foreign Intelligence Surveillance Act of 1978 Amendments of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (2008) (“FAA”). To the extent that the government conducted surveillance pursuant to the FAA, the defendants reserve the right to challenge the use of the results of any such surveillance.

<sup>2</sup> *See, e.g.*, FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. Rep. No. 94-755, 94<sup>th</sup> Cong., 2d Sess. (1976); *Commission on CIA Activities Within the United States*, Report to the President

for foreign intelligence gathering within the confines of the United States in response to civil liberties concerns and the gap in the law noted by the Supreme Court in *United States v. United States District Court (Keith, J.)*, 407 U.S. 297, 308-09 (1972).

Through FISA, Congress attempted to limit the ability of the Executive Branch to engage in abusive or politically-motivated surveillance. FISA constituted Congress' attempt to balance the "competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the Nation, and the requirements of the Fourth Amendment." H.R. Rep. No. 95-1283, at 15. FISA's provisions therefore represented a compromise between civil libertarians seeking preservation of Fourth Amendment and privacy rights, and law enforcement agencies citing the need for monitoring agents of a foreign power operating in the United States. *See In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (FISA "was enacted in 1978 to establish procedures for the use of electronic surveillance in gathering foreign intelligence information. . . . The Act was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties") (quotation omitted).

Important differences exist between the standards for a FISA warrant and that issued under the Fourth Amendment or Title III of the U.S. Criminal Code. The "probable cause" required under FISA is merely that the target qualifies as an "agent of a foreign power," 50 U.S.C. § 1801(b), who will use the electronic device subject to electronic surveillance, or owns, possesses, uses, or is in the premises to be searched, *see* 50 U.S.C. §§ 1805(a)(3) & 1824(a)(3),

---

(1975) (commonly referred to as the "Rockefeller Commission Report"). *See also United States v. Belfield*, 692 F.2d 141, 145 (D.C. Cir. 1982) ("[r]esponding to post-Watergate concerns about the Executive's use of warrantless electronic surveillance, Congress, with the support of the Justice Department, acted in 1978 to establish a regularized procedure for use in the foreign intelligence and counterintelligence field").

and not that a crime has been, or is being, committed.

In that context, FISA establishes procedures for surveillance of foreign intelligence targets, whereby a federal officer acting through the Attorney General may obtain judicial approval for conducting electronic surveillance for foreign intelligence purposes. The FISA statute created a special FISA Court – the Foreign Intelligence Surveillance Court (hereinafter “FISC”) – to which the Attorney General must apply for orders approving electronic surveillance of a foreign power, or an agent of a foreign power, for the purpose of obtaining foreign intelligence information. *See* 50 U.S.C. §§1802(b), 1803 & 1804.<sup>3</sup> In addition, the Attorney General must review the application and determine whether it satisfies the criteria and requirements set forth in FISA. § 1804(d); *see also* § 1805(a)(1).

Regarding the judicial component of the FISA process, in considering an application for electronic surveillance pursuant to FISA, the Court should reject the application unless the application meets the following criteria sufficient to permit the Court to make the requisite findings under §1805(a):

- (i) that the application was made by a federal officer and approved by the Attorney General;
- (ii) that there exists probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and . . . each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or agent of a foreign power[;]”

---

<sup>3</sup> The FISC consists of eleven judges (previously seven prior to amendments adopted as part of the The USA PATRIOT Act) who individually hear government applications. *See* 50 U.S.C. § 1803.

- (iii) that the proposed minimization procedures meet the definition of minimization procedures under §1801(h); and
- (iv) that the application contains all required statements and certifications.

Also, in accordance with §1805(a)(4), if a target is a “United States person,” the FISC must determine whether the “certifications” under §1804(a)(6)(E) – namely that the information sought is “the type of foreign intelligence information designated,” and the information “cannot reasonably be obtained by normal investigative techniques” – are “not clearly erroneous.” In addition, §1805(a)(2)(A) provides “that no United States person may be considered a foreign power . . . solely upon the basis of activities protected by the first amendment . . .”

FISA authorizes any “aggrieved person” to move to suppress evidence obtained or derived from an electronic surveillance on the grounds that “the information was unlawfully acquired” or “the surveillance was not made in conformity with an order of authorization or approval.” §§ 1806(e)(1) & (2); 1825(f). FISA defines “aggrieved person” as “a person who is the target of electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” § 1801(k).

FISA also permits evidence generated in intelligence investigations to be used in criminal prosecutions. §§ 1806(b) & 1825(c). However, if a significant purpose of the surveillance is not to obtain foreign intelligence information but rather for the purpose of a criminal investigation, obtaining that evidence without complying with the Fourth Amendment violates the Constitution. *See* § 1804(a)(6)(B).

## **2. Challenges to the Admissibility of FISA-Generated Evidence**

Because Ms. Jama and Ms. Dhirani have been notified that their communications and

property have been the subject of FISA surveillance and searches, they are “aggrieved person[s]” under § 1806(k). Nonetheless, defense counsel in this case have not been provided with the FISA applications that resulted in the surveillance and searches at issue.

While aggrieved criminal defendants can move to suppress FISA-generated evidence, §1806(f) provides that if the Attorney General files an affidavit that “disclosure or an adversary hearing would harm the national security of the United States,” the court deciding the motion must consider the application and order for electronic surveillance *in camera* to determine whether the surveillance was conducted lawfully. Accordingly, FISA “requires the judge to review the FISA materials *ex parte in camera* in every case” to “decide whether any of those materials must be disclosed to defense counsel.” *United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014).

The statute also adds that, “[i]n making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” 50 U.S.C. § 1806(f). Alternatively, § 1806(g) provides that “[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.”

The lack of access to the underlying FISA applications presents a significant impediment to asserting a challenge to FISA surveillance with particularity. As the Fourth Circuit has recognized in an analogous context, the burden to be specific with respect to the basis for suppression must be relaxed when the information supporting the motion is held uniquely by the

government. *Cf. United States v. Moussaoui*, 382 F.3d 453, 472 (4th Cir. 2004), *citing United States v. Valenzuela-Bernal*, 458 U.S. 858, 870-71, 873 (1982).

**1. *Grounds Upon Which the FISA Applications May Fail to Establish the Requisite Probable Cause***

**a. *The Elements of Probable Cause Under FISA***

Before authorizing FISA surveillance, the FISA Court must find, *inter alia*, probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power.” §1805(a)(2)(A). The Supreme Court has reiterated the long-standing rule that criminal probable cause requires “a reasonable ground for belief of guilt,” and that “the belief of guilt must be particularized with respect to the person to be searched or seized.” *Maryland v. Pringle*, 540 U.S. 366, 371 (2003). Under FISA, though, unlike with respect to a traditional warrant, the probable cause standard is directed *not* at the target’s alleged commission of a crime, but at the target’s alleged status as “a foreign power or an agent of a foreign power.”

**b. *The “Agent of a Foreign Power” Requirement***

Consequently, this Court must initially determine, with respect to each application for FISA electronic surveillance of Ms. Jama and Ms. Dhirane, whether the application established a reasonable, particularized ground for belief that the defendants qualified as an agent of a foreign power. §§1805(a)(2)(A) & 1801(b)(2)(C) & (E).

Here, absent an opportunity to review the applications for any of the surveillance at issue, defense counsel cannot specify whether the allegations asserting that the defendants were an “agent of a foreign power” were sufficient to satisfy FISA. Among FISA’s definitions of “agent of a foreign power,” §1801(b)(2)(C) provides that the term includes: “any person . . . who



*knowingly* engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power.” (Emphasis added).

If that provision was, in fact, the basis for the FISA applications, the statute requires the presentation of evidence establishing probable cause that the defendant or the relevant third-party target *knowingly* engaged in some type of international terrorism, and that the defendants *knew* that their activities were assisting “international terrorism”.

**c. *The Nature and Origins of the Information In the FISA Applications***

Again, unlike the case with traditional warrants, non-disclosure of the FISA applications denies the defense the ability to contest the accuracy or reliability of the underlying information used to satisfy FISA’s version of probable cause. As a result, absent such disclosure the defendants can request only that the Court review the FISA applications cognizant of certain factors and principles.

**i. *The Limits of “Raw Intelligence”***

For example, foreign intelligence information is often in the form of “raw intelligence,” and not vetted in the manner typical of information law enforcement agents supply in ordinary warrant applications, *i.e.*, that the information emanated from a source that was reliable and/or had a verifiable track record, or was independently corroborated.

Such raw intelligence is often not attributed to *any* specific source, and its genesis can be multiple-level hearsay, rumor, surmise, and rank speculation. Also, the motivation driving sources of raw intelligence to impart information is usually not nearly as transparent as in conventional criminal justice circumstances. As a result, the dangers of deception and disinformation are significantly enhanced.

Those limitations on the accuracy and reliability of raw intelligence are aggravated when the potential location – Somalia, a nation afflicted by chaos, and to which the U.S. government has very limited formal access – and context – often military and susceptible to the “fog of war” – reduce the possibility of meaningful corroboration or verification.

**ii. *Illegitimate and/or Illegal Sources of Information***

There is also the danger that the information in FISA applications, whether or not attributed to a particular source, was generated by illegal means such as warrantless wiretapping or constitutionally infirm FISA amendments that have yet to be challenged in criminal cases. In that context, the government should be compelled to disclose whether information in the FISA applications, or which was used to obtain information that appears in the applications, or was used in the investigation in this case in any fashion, originated from such illegitimate means. *Cf. Gelbard v. United States*, 408 U.S. 41 (1972) (in prosecution for contempt for refusal to testify, grand jury witness entitled to invoke as a defense statutory bar against use of evidence obtained via illegal wiretap as basis for questions in grand jury).

**(A) *The Warrantless Terrorist Surveillance Program***

For example, the government should be required to disclose whether any of the defendants’ communications were intercepted pursuant to the Terrorist Surveillance Program (hereinafter “TSP”), a warrantless wiretapping program instituted in 2001. *But cf. United States v. Abu Ali*, 528 F.3d 210, 257 (4th Cir. 2008) (affirming district court’s conclusion that disclosure of TSP was not warranted based on *ex parte* review of government justification). The government should further be compelled to disclose whether any communications intercepted pursuant to the TSP contributed to the FISA applications or the search warrant applications, or to

the investigation of this case in any manner.

**(B) *Surveillance Pursuant to the FISA Amendments Act***

The Court should also examine whether any portion of the FISA electronic surveillance was requested and conducted pursuant to the authority provided in 50 U.S.C. §1881a, enacted in 2008 as part of the FISA Amendments Act of 2008, Pub. L. No. 110-261 (2008), or whether any information in the FISA applications was the product of surveillance authorized under the FAA.

Congress amended FISA, effective Summer 2008, to allow for the collection of some electronic communications – ostensibly international in character, but which could include a domestic component (*i.e.*, one party within the United States) – without a traditional FISA warrant, but rather on advance court approval of targeting methods rather than designation of a particular target based on individualized probable cause. Those provisions, codified at 50 U.S.C. §1881a, raise constitutional issues different from those implicated by the pre-existing FISA provisions. The government should not have any legitimate interest in obscuring the authority pursuant to which it conducted FISA surveillance herein; indeed, refusal by the government to so disclose would deny the defendants a fair trial by depriving them of any meaningful opportunity to contest the acquisition and admissibility of evidence that may have been obtained unlawfully. Accordingly, the Court should examine the nature, genesis, and provenance of the information in the FISA application, and compel the government to disclose whether any such information was the product of warrantless electronic surveillance (either via the TSP or any other program), or of such surveillance authorized pursuant to the FAA (§1881a).

**d. *FISA’s Prohibition On Basing Probable Cause Solely On a “United States Person’s” Protected First Amendment Activity***

The statute includes an additional restriction for electronic surveillance of a “United States person,” as it prohibits finding probable cause for such a target based solely upon First Amendment activities. In making that probable cause determination, the statute directs “[t]hat no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment . . .” §1805(a)(2)(A).

Accordingly, if the target participated in First Amendment activities such as expressing support, urging others to express support, gathering information, distributing information, raising money for political causes, or donating money for political causes, these activities cannot serve as a basis for probable cause for a FISA warrant. The statute reaches only material support coordinated with or under the direction of a designated foreign terrorist organization. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 31-32 (2010) (“Independent advocacy that might be viewed as promoting the group’s legitimacy is not covered.”).

**2. *The FISA Applications May Contain Intentional or Reckless Falsehoods or Omissions In Contravention of Franks v. Delaware, 438 U.S. 154 (1978)***

The Supreme Court’s landmark decision in *Franks v. Delaware*, 438 U.S. 154 (1978), established the circumstances under which the target of a search may obtain an evidentiary hearing concerning the veracity of the information set forth in a search warrant affidavit. As the Court in *Franks* instructed, “where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statements necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.” *Id.* at 156-57.

The *Franks* opinion also sets a similar standard for suppression following the evidentiary hearing:

in the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

*Id.*, at 156; *see United States v. Blackmon*, 273 F.3d 1204, 1208-10 (9th Cir. 2001) (applying *Franks* to Title III wiretap application); *United States v. Meling*, 47 F.3d 1546, 1553-56 (9th Cir. 1995) (same); *United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (suggesting that *Franks* applies to FISA applications under Fourth and Fifth Amendments). *See also United States v. Hammond*, 351 F.3d 765, 770-71 (6th Cir. 2003) (applying *Franks* principles).

The *Franks* principles apply to omissions as well as to false statements. *See, e.g., United States v. Carpenter*, 360 F.3d 591, 596-97 (6th Cir. 2004); *United States v. Atkin*, 107 F.3d 1213, 1216-17 (6th Cir. 1997). Omissions will trigger suppression under *Franks* if they are deliberate or reckless, and if the search warrant affidavit, with omitted material added, would not have established probable cause.

As noted above, without the opportunity to review the applications, the defendants cannot point to or identify any specific false statements or material omissions in those applications. *See Daoud*, 755 F.3d at 493 (Rovner, J., concurring) (explaining difficulty of reconciling *Franks* with denying access to FISA warrant applications, and concluding that “[w]ithout access to the FISA application, it is doubtful that a defendant could ever make a preliminary showing sufficient to trigger a *Franks* hearing.”). Although that lack of access prevents defense counsel from making

the showing that *Franks* ordinarily requires, counsel notes that the possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions is hardly speculative.

For instance, in 2002, in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (FISC), *rev'd on other grounds sub nom., In re Sealed Case*, 310 F.3d 717 (FISCR 2002),<sup>4</sup> the FISC reported that beginning in March 2000, the Department of Justice (hereinafter “DoJ”) had come “forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts,” including:

- “75 FISA applications related to major terrorist attacks directed against the United States” contained “misstatements and omissions of material facts.” 218 F. Supp. 2d at 620-21;
- the government’s failure to apprise the FISC of the existence and/or status of criminal investigations of the target(s) of FISA surveillance; and
- improper contacts between criminal and intelligence investigators with respect to certain FISA applications. *Id.*

According to the FISC, “[i]n March of 2001, the government reported similar misstatements in another series of FISA applications . . .” *Id.* at 621. Nor were those problems isolated or resolved by those revelations. A report issued March 8, 2006 by the DoJ Inspector General stated that the FBI found apparent violations of its own wiretapping and other

---

<sup>4</sup> “FISCR” refers to the Foreign Intelligence Court of Review, which is the appellate court for the FISC, and is comprised of three federal Circuit judges. The FISCR’s 2002 decision in *In re Sealed Case* marked its first case since enactment of FISA in 1978.

intelligence-gathering procedures more than 100 times in the preceding two years, and problems appear to have grown more frequent in some crucial respects. *See* Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act, March 8, 2006.

The report characterized some violations as “significant,” including wiretaps that were much broader in scope than authorized by a court (“over-collection”), and others that continued for weeks and months longer than authorized (“overruns”). *Id.* at 24-25. FISA-related overcollection violations constituted 69% of the reported violations in 2005, an increase from 48% in 2004. *See* DoJ IG Report, at 29. The total percentage of FISA-related violations rose from 71% to 78% from 2004 to 2005, *id.* at 29, although the amount of time “over-collection” and “overruns” were permitted to continue before the violations were recognized or corrected decreased from 2004 to 2005. *Id.* at 25.

Thus, a *Franks* hearing, and disclosure of the underlying FISA materials, are necessary in order to permit the defendants the opportunity to prove that the affiants before the FISC intentionally or recklessly made materially false statements and omitted material information from the FISA applications.

### **3. *The Collection of Foreign Intelligence Information May Not Be a Significant Purpose of the FISA Surveillance***

If the investigation, and purpose of the FISA surveillance, was criminal in nature, all of the evidence derived from the FISA surveillance of the defendants should be suppressed because the applications failed to adhere to FISA’s requirements, or in the alternative to seek appropriate authority under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 99 2510-2520 (1982), rather than under FISA.

**4. *The FISA Applications May Not Have Included the Required Certifications***

The Court should review the FISA applications to determine whether they contain all certifications required by §1804(a)(6). As the Ninth Circuit has declared in the Title III context, “[t]he procedural steps provided in the Act require ‘strict adherence,’” and “utmost scrutiny must be exercised to determine whether wiretap orders conform to [the statutory requirement].”

*Blackmon*, 273 F.3d at 1207, *quoting United States v. Kalustian*, 529 F.2d 585, 588-9 (9th Cir. 1975).

In addition, the Court should examine two certifications with particular care – (i) that the information sought is “the type of foreign intelligence information designated,” and (ii) that the information “cannot reasonably be obtained by normal investigative techniques.” *See* §1804(a)(6)(E). Particularly if the target of the wiretap is a “United States person” (such as the defendants), these two certifications must be measured by the “clearly erroneous” standard. *See* §1805(a)(4).

As the Ninth Circuit has observed in relation to the similar provision in Title III, 18 U.S.C. § 2518(1)(e), “the necessity requirement ‘exists in order to limit the use of wiretaps, which are highly intrusive.’” *Blackmon*, 273 F.3d at 1207, *quoting United States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000) (internal quotation omitted). The necessity requirement “ensure[s] that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the [information sought].” *Id.*

The Court should also carefully examine the dates, in sequence, of all FISA orders in this case to determine whether there were any lapses of time during which wiretapping continued. The statutory scheme contemplates that when a FISA order expires and the government wishes to



continue the wiretap, the expiring order must be replaced by an extension order, which, in turn, may be obtained only on the basis of a proper FISA application. *See* §1805(d)(1) & (2).

FISA surveillance that continues past the expiration date of the FISA order that originally authorized it is just as unauthorized as a wiretap that is initiated without any FISA order at all. Should the Court order the government to disclose the FISA orders in this case to defense counsel, the defense will be able to assist the Court in matching up all of the FISA orders by date.

**5. *The FISA Applications, and the FISA Surveillance, May Not Have Contained or Implemented the Requisite Minimization Procedures***

In order to obtain a valid FISA order, the government must include in its application a “statement of the proposed minimization procedures.” §1804(a)(4). The purpose of these minimization procedures is to (i) ensure that surveillance is reasonably designed to minimize the acquisition and retention of private information regarding people who are being wiretapped; (ii) prevent dissemination of non-foreign intelligence information; and (iii) prevent the disclosure, use, or retention of information for longer than seventy-two hours unless a longer period is approved by Court order. §1801(h).

FISA surveillance involves particularly intrusive electronic surveillance. Indeed, it typically occurs on a continuance 24-hour basis, as the Title III principle of “pertinence” is not applicable. Instead, *all* conversations are captured, with minimization occurring later and in other forms. Accordingly, minimization in the FISA context is critically important.

One court has reasoned that in FISA the privacy rights of individuals are ensured not through mandatory disclosure of FISA applications, but

through its provisions for in-depth oversight of FISA surveillance  
*by all three branches of government* and by a statutory scheme that

to a large degree centers on *an expanded conception of minimization* that differs from that which governs law-enforcement surveillance.

*United States v. Belfield*, 692 F.2d 141, 148 & n. 34 (D.C. Cir. 1982) (footnote omitted), *quoting* Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs are Doing Their Job*, 12 RUTGERS L.J. 405, 408 (1981) (emphasis added).

Here, the government has provided an incredibly large amount of products of surveillance. It is possible that the FISA application did not contain adequate minimization procedures or, if it did, that those procedures were not followed. In order to determine whether there were adequate minimization procedures, and that the government complied therewith, defense counsel must be provided with the FISA applications, orders, and related materials.

**C. *The Underlying FISA Applications and Other Materials Should Be Disclosed to Defense Counsel to Enable Them to Assist the Court, and On Due Process Grounds***

**1. *Disclosure of FISA Materials to the Defense Pursuant to §1806(f)***

According to FISA's legislative history, disclosure may be "necessary" under §1806(f) "where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) [*quoting* S. Rep. No. 701, 95th Cong., 2d Sess. 64 (1979)]; *see, e.g., United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987) (same); *United States*

*v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same).

There are ample justifications for disclosure of the FISA applications in this case which would permit defense counsel an opportunity to demonstrate that the requisite probable cause with respect to the issue of knowledge was lacking, that with respect to the defendants, “United States person[s],” the alleged “activities” fell within the protection of the First Amendment and, thus, could not be used as a basis for probable cause in any event, and that the information in the applications was either unreliable or obtained via illegal means. Disclosure would also afford defense counsel an opportunity to identify procedural irregularities.

In addition, counsel for the defendants possess the requisite level of security clearance for this case, and have received Top Secret-SCI clearances in other cases. The Court therefore could issue an appropriate Protective Order that would provide elaborate protection for classified information, and which would permit such materials to be disclosed to defense counsel but not to the defendants. *See* Classified Information Procedures Act (hereinafter “CIPA”), 18 U.S.C. App. III, at §3.

Thus, while no court in the history of FISA has ordered disclosure of FISA applications, orders, or related materials, *see, e.g., In re Grand Jury Proceedings*, 347 F.3d 197, 203 (7th Cir. 2003) (citing cases); *United States v. Sattar*, 2003 U.S. Dist. LEXIS 16164, at \*19 (S.D.N.Y. Sept. 15, 2003) (same), disclosure should occur in this case. Indeed, the existence of §1806(f) is an unambiguous declaration that Congress intended for courts to grant disclosure in appropriate cases. If §1806(f) is to be rendered meaningful at all, and not be rendered superfluous and entirely inert, it should apply in this case.

## **2. Disclosure of FISA Materials to the Defense Pursuant to §1806(g)**

Even if the Court were to decline to find that disclosure of FISA-related materials to the defense is appropriate under §1806(f), the defense would still be entitled to disclosure of the FISA applications, orders, and related materials under §1806(g), which expressly incorporates the Fifth Amendment Due Process Clause, and provides that “[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure.*” 50 U.S.C. §1806(g) (emphasis added). *See also United States v. Spanjol*, 720 F. Supp. 55, 57 (E.D. Pa. 1989) (“[u]nder FISA, defendants are permitted discovery of materials only to the extent required by due process. That has been interpreted as requiring production of materials mandated by [*Brady*], essentially exculpatory materials”).

**3. Ex Parte Proceedings To Address this Motion Are Antithetical to the Adversary System of Justice**

Lack of disclosure would render the proceedings on the validity of the FISA electronic surveillance *ex parte*, as the challenges on the defendants’s behalf would be made without access to documents and information essential to the determination of his motion. Such proceedings are antithetical to the adversary system that is the hallmark of American criminal justice.

As an initial matter, the adversary nature of our system of criminal justice warrants participation by the defense in the actual conversation regarding the legality of surveillance used to prosecute the defendants. Indeed, “Article III of the Constitution limits federal-court jurisdiction to ‘Cases’ and ‘Controversies.’ Those two words confine ‘the business of federal courts to questions presented in an adversary context and in a form historically viewed as capable of resolution through the judicial process.’” *Massachusetts v. E.P.A.*, 549 U.S. 497, 516 (2007)

(quoting *Flast v. Cohen*, 392 U.S. 83, 95 (1968)). Although proceedings to obtain judicial authorization for searches and surveillance by law enforcement are an exception to this rule, challenges to such proceedings and the resulting searches and surveillance are not.

Moreover, as the Supreme Court has recognized, “[f]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.” *United States v. James Daniel Good Real Property, et al.*, 510 U.S. 43, at 55 (1993) (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). See also *United States v. Madori*, 419 F.3d 159, 171 (2d Cir. 2005), citing *United States v. Arroyo-Angulo*, 580 F.2d at 1145 (closed proceedings “are fraught with the potential of abuse and, absent compelling necessity, must be avoided”) (other citations omitted).<sup>5</sup>

Indeed, “[f]or more than a century the central meaning of procedural due process has been clear: ‘Parties whose rights are to be affected are entitled to be heard; and in order that they may enjoy that right they must first be notified.’ It is equally fundamental that the right to notice and an opportunity to be heard ‘must be granted at a meaningful time and in a meaningful manner.’” *Fuentes v. Shevin*, 407 U.S. 67, 80 (1972) (quoting *Baldwin v. Hale*, 1 Wall. 223, 233, 17 L.Ed. 531 (1864)).

In *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004), the Second Circuit

---

<sup>5</sup> Conversely, as Judge Learned Hand said in *United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950), *cert. denied*, 342 U.S. 920 (1952), “[f]ew weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which it seeks to forfeit the liberty of its citizens.”

reemphasized the importance of open, adversary proceedings, declaring that “[p]articularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other.” 389 F.3d at 322-23 (*citing McGrath*, 341 U.S. at 171 n. 17 (Frankfurter, J., *concurring*)), which noted that “the duty lying upon every one who decides anything to act in good faith and fairly listen to both sides . . . always giving a fair opportunity to those who are parties in the controversy for correcting or contradicting any relevant statement prejudicial to their view”) (citation and internal quotation marks omitted).

As the Ninth Circuit observed in the closely analogous context of a secret evidence case, “[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations.’ . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error.” *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1069 (9<sup>th</sup> Cir. 1995) (*quoting* District Court); *see, e.g., id.* at 1070 (noting “enormous risk of error” in use of secret evidence).

Similarly, in the Fourth Amendment context, including in relationship to electronic surveillance, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman v. United States*, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to the prosecution case against the defendants. The Court rejected the government's suggestion that the district court make that determination *in camera* and/or *ex parte*.

The Court observed that

[a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

*Id.* at 182.

In ordering disclosure of improperly recorded conversations, the Court declared:

[a]dversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

*Id.* at 184.

Likewise, the Court held in *Franks v. Delaware*, 438 U.S. 154 (1978), that a defendant, upon a preliminary showing of an intentional or reckless material falsehood in an affidavit underlying a search warrant, must be permitted to attack the veracity of that affidavit. The Court rested its decision in significant part on the inherent inadequacies of the *ex parte* nature of the procedure for issuing a search warrant, and the contrasting enhanced value of adversarial proceedings:

the hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily *ex parte*, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an *ex parte* inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-

search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

438 U.S. at 169.

The same considerations that the Supreme Court found compelling in *Alderman* and *Franks* militate against *ex parte* procedures in the FISA context. Indeed, the lack of any authentic adversary proceedings in FISA litigation more than likely accounts for the government's perfect record in defending FISA and FISA-generated evidence. After all, denying an adversary access to the facts constitutes an advantage as powerful and insurmountable as exists in litigation.

As the FISC itself has acknowledged, for example, without adversarial proceedings, systematic executive branch misconduct – including submission of FISA applications with “erroneous statements” and “omissions of material facts” – went entirely undetected by the courts until the FISC directed that the Department of Justice review FISA applications and submit a report to the FISC. *See In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp.2d at 620-21, *rev'd on other grounds*, 310 F.3d 717 (FISCR 2002).

However, as discussed above, the complete deference now required of the courts toward the executive with respect to FISA renders any such “in-depth oversight” and “expanded conception of minimization” entirely illusory. As a result, §§1806(f) & (g), and the disclosure they authorize, assume significantly greater meaning and importance in evaluating the validity of FISA applications. Also, as noted above, the defendants' counsel possess the requisite security clearance to view the material, thereby further eliminating any justification for non-disclosure, or



any claim that such limited, safe disclosure presents any danger to national security.

Moreover, the Court's review *in camera* is not a substitute for defense counsel's participation. As the Supreme Court recognized in *Alderman*, "[i]n our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate." 394 U.S. at 184; *see also Franks v. Delaware*, 438 U.S. 154, 169 (1978) (permitting adversarial proceeding on showing of intentional falsehood in warrant affidavit because the magistrate who approves a warrant *ex parte* "has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations").

Accordingly, either under §1806(f), §1806(g), and/or the Due Process clause, disclosure of the FISA materials is authorized and appropriate in this case.

### **Conclusion**

For the foregoing reasons, Ms. Jama and Ms. Dhirane respectfully request that the Court suppress all information and evidence obtained pursuant to the FISA in this case.

Respectfully submitted,  
MUNA OSMAN JAMA  
By Counsel,  
Jeremy C. Kamens  
Acting Federal Public Defender

By: \_\_\_\_\_/s/  
Jeremy C. Kamens  
Va. Bar #41596  
Acting Federal Public Defender  
Whitney E.C. Minter  
Va. Bar # 47193  
Assistant Federal Public Defender  
Attorneys for Muna Jama  
1650 King Street, Suite 500  
Alexandria, Virginia 22314  
(703) 600-0855 (telephone)  
(703) 600-0880 (facsimile)  
Whitney\_Minter@fd.org (email)

**CERTIFICATE OF SERVICE**

I hereby certify that on December 11, 2015, I will electronically file the foregoing pleading with the Clerk of the Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

James Gillis, Esq.  
Assistant United States Attorney  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
(703) 299-3700  
james.p.gillis@usdoj.gov

Pursuant to the Electronic Case Filing Policies and Procedures, a courtesy copy of the foregoing pleading will be delivered to Chambers within one business day of the electronic filing.

By: \_\_\_\_\_/s/  
Geremy C. Kamens  
Va. Bar # 41596  
Acting Federal Public Defender  
Whitney E.C. Minter  
Va. Bar # 47193  
Assistant Federal Public Defender  
Attorneys for Muna Jama  
1650 King Street, Suite 500  
Alexandria, Virginia 22314  
(703) 600-0855 (telephone)  
(703) 600-0880 (facsimile)  
Whitney\_Minter@fd.org (email)